Novel DCT based watermarking scheme for digital images

Neminath Hubballi, Kanyakumari D P,
Dept of Computer Science,Indian Institute of Technology Guwahati
neminath@iitg.ernet.in
Dept of Information Science,GMIT, Davanagere,karnataka
kanya.dpoojar@gmail.com

Abstract

There is an ever growing interest in copyright protection of multimedia content, thus digital watermarking techniques are widely practiced. Due to the internet connectivity and digital libraries the research interest of protecting digital content watermarking is extensively researched. In this paper we present a novel watermark generation scheme based on the histogram of the image and apply it to the original image in the transform(DCT) domain. Further we study the performance of the watermark against some common attacks that can take place with images. Experimental results show that the embedded watermark is imperceptible and image quality is not degraded.

I. Introduction

Internet has given great help to mankind at the same time brought up serious security issues to the forefront. This widespread connectivity of computers across the globe makes it feasible to access the information from any place. As connectivity increases the risk associated with the security of data or information also scales up. This development of web technology makes the transfer of digital content more pervasive. To protect the ownership of such digital content watermarking[8], [1] techniques are used. Watermark is an invisible mark(another piece of digital data) inserted into original digital content and is not easy to erase. The security of watermark depends on the secrete key used for generation and embedding of watermark. In general there is a trade off between the embedding strength(the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images. Some of the desired characteristics of watermarking techniques are

- Imperceptibility - It should not be possible to find the presence of watermark from bare eyes.
- Key requirement - Different keys should produce different watermarks.
- Reliable detection - It should be possible to detect the watermark with high degree of reliability given the key.
- Robustness - It should tolerate some of the common image processing attacks.

In literature watermarking algorithms are classified into two categories. a) Fragile: These algorithms are sensitive to changes that are made to the digital signal and identify where the change has occurred.
b) Robust: These algorithms ensure that the image processing operations do not erase the embedded watermark signal. Several watermarking approaches appear in literature. Most of these techniques work in transform domain such as DFT, DWT and DCT although there are many methods which work in spatial domain. Many of the algorithms proposed meet the imperceptibility requirement quite easily but robustness to different image processing attacks is the key challenge and the algorithms in literature addressed only a subset of attacks. Recently a clustering based technique is applied in[7]. In [5] a method to watermark only face region is proposed. In a more similar technique [3] proposes identifying robust regions in the image segments and watermarking the most robust segments. There are some visible watermarking techniques also present in the literature which have different requirements as compared to the conventional techniques [6] is such a technique. A more detailed study on different watermarking techniques can be found in[2].

In this paper we propose a novel a DCT transform based watermarking scheme which is robust against many common image attacks and experimental results verify this. The paper is organized as follows. Section II discuses the proposed method. The section III provides the experimental results and discussion. Finally the last section provides the concluding remarks.

© 2010 ACEEE
DOI: 01.ijsip.01.01.03

II. PROPOSED METHOD

The proposed algorithm is a transform domain (frequency domain) watermarking scheme and works by modifying the DCT(Discrete Cosine Transform) coefficients. The watermark is content based i.e generated from the image itself and no external signal source is used as watermark. Hence we need a way to generate the watermark sequence from the image which in our case is a binary digit. The step by step procedure for generating the watermark data(signal) is given bellow. It is to be noticed that the binary sequence generation is done with spatial domain information but the embedding of watermark done in transform domain.

A. Watermark generation

The watermark to be embedded into image is generated as follows.

- Histogram of the image to be watermarked is generated and the mean of the histogram is calculated. Let H_m be the mean of histogram.
- The gray scale threshold of the image is calculated using Otsu's method[4]. Let G_t be the gray level threshold of the image which is a number between 0 and 1.
- Downscale the mean histogram H_m by multiplying it with G_t. Let this value be T_h.
- Divide the original image into blocks

$$Xb = Xb(k, l),\ 0 \le k \le N\,1 / 8, 0 \le l < N2 / 8 \quad (1)$$

where N_1 and N_2 are the number of rows and columns of image.

- Calculate the mean of the blocks as

$$Mb(k,l) = 1/64 \sum_{i=1}^{7} \sum_{j=1}^{7} X(K*8+I, l*8+j) \quad (2)$$

- Compare T_h with $M_b(k; l)$ and generate the binary sequence as

if $M_b(k; l) > T_h$ then

$W(k; l) = 0$

else

$W(k; l) = 1$

Thus computed matrix W is a binary pattern of 0's and 1's which is the watermark. It is to be noted that this watermark is generated from some operations applied on image blocks itself rather than taking from external source, hence the name content based watermark. This watermark is embedded into the DCT coefficients of image blocks and the procedure for embedding the watermark is described in the next section.

B. Watermark embedding

The watermark generated from the original image is embedded in the Discrete Cosine Transform(DCT) domain to the image itself. We divide the image into blocks of size 8X8 and apply the DCT on each block which is given by the equation 3, thus transforming a block of time domain coefficients into of the same size frequency domain coefficients. The mid frequency coefficients are as identified by the bellow matrix are altered according to the equation 4. In literature the mid frequency coefficients are normally chosen for adding watermark, this is because these coefficients are not altered significantly when the image is compressed and filtered. Hence we used the same method here.

$$C(u,v) = a(u)a(v) \sum_{X=0}^{N-1} \sum_{y=0}^{N-1} f(x,y)$$
$$\cos[\prod (2x + 1)u / 2N] \cos[\prod (2y + 1)u / 2N] \quad (3)$$

0	0	0	1	1	1	1	0
0	0	1	1	1	1	0	0
0	1	1	1	1	0	0	0
1	1	1	1	0	0	0	0
1	1	1	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

$$Y_w(k,l) = X(k,l) + aX(k,l)\, W(k,l) \quad (4)$$

B. Watermark extraction

To verify the presence of watermark, original image is required. In the first step the effect of watermarking is undone on the suspicious image. After that the watermark pattern is calculated from this image using the steps described to generate the watermark pattern. The undoing is defined using the equations 5 and 6.

$$Y_c(k,l) = Y_w(k,l) \text{ if } W(k,l) \quad (5)$$

Else

$$Y_c(k,l) = 1/(1+a) Y_w(k,l) \quad (6)$$

© 2010 ACEEE
DOI: 01.ijsip.01.01.03

ACEEE

III. EXPERIMENTS AND DISCUSSION

The experimentation is done using the standard Lenna image. We used matlab image processing toolbox for performing experiments. The watermark signal is generated according to
the steps described in section II and for implicity we can assume the number of rows and columns are exact multiples of 8(as we are dividing into blocks of size 8 X 8). Fig 1 shows the original image which is used for watermarking, where as Fig 2 shows the watermarked image and Fig 3 shows the watermark extracted image. From the three figures we notice that, there is no great visual distortion with embedding process. To study the robustness the watermarking method the image is subjected to various image processing attacks. The first being the JPEG compression, where low frequency components of the image are normally zeroed out. Since the middle frequency components are normally not distorted to a great extent our method gives better resilience to compression. To study the behavior of watermark under the JPEG compression we subjected the image for compression with three different standardized quantization matrices. The quantization matrices are shown in the table I II and III.

TABLE I

3	2	2	3	5	8	10	2
2	2	3	4	5	12	12	11
3	3	3	5	8	11	14	11
3	3	4	6	10	17	16	12
4	4	7	11	14	22	21	15
5	7	11	13	16	12	23	18
10	13	16	17	21	24	24	21
4	18	19	20	22	20	20	20

The following table III gives the performance of watermarking scheme with the standard Lena image of size 256 X 256 against the compression and with or without median filtering applied with a 3 x 3 window. Peak Signal to Noise Ratio (PSNR) and Normalized Cross Correlation (NCC) are used as the criteria for measurement.

Fig. 1. Original Image .

Fig. 2. Watermarked Image .

Fig. 3. Watermark exctracted Image .

TABLE II
QUANTIZATION MATRIX Q2

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	113
49	64	78	87	103	121	120	101
72	92	95	98	112	100	100	99

© 2010 ACEEE
DOI: 01.ijsip.01.01.03

ACEEE

The following table III shows the effects of blurring the image using a Gaussian low pass filter and sharpening with UnSharp Mask filter. An NCC of 0.9999 was observed when there is no attack on the image.

TABLE III

QUANTIZATION MATRIX Q3

52	55	61	66	70	61	64	73
63	59	66	90	109	85	69	72
62	59	59	113	113	113	66	73
63	58	71	122	154	106	70	69
67	61	68	104	126	88	68	70
79	65	60	70	77	68	58	58
85	71	64	59	55	61	61	83
87	79	69	68	68	76	76	94

TABLE IV

PERFORMANCE AGAINST QUANTIZATION

Q Matrix	PSNR without filtering	PSNR with filtering	NCC without filtering	NCC with filtering
Ql	45.03	32.76	0.7814	0.9654
Q2	30.79	28.05	0.9788	0.9883
Q3	46.23	32.56	0.7300	0.9883

TABLE V

PERFORMANCE AGAINST BLURRING AND SHARPENING

Operation	PSNR	NCC
Blurring	31.13	0.9977
Sharpening	24.82	0.9826

IV. CONCLUSION

In this paper we presented a novel DCT based approach for watermarking digital still images and evaluated the performance of the scheme with some possible image processing attacks. Experiments revealed a good resilience against such attacks. Moreover the authorization procedure is simple and fast also allows easy extraction.

REFERENCES

[1] H. Berghel and L. O'Gorman, Protecting ownership rights through digital watermarking, IEEE Computer Magazine (July-1996), 101–103.

[2] Edin Muharemagic, Survey of watermarking techniques and applications., Department of computer science and engineering , Florida Atlantic University.

[3] Athanasios Nikolaids and ioannis Pitas, Region-based image watermarking, IEEE Transactions on Image Processing 10 (November , 2001), 1726–1740.

[4] N. Otsu, A threshold selection method for gray-level histograms, IEEE Transactions on Systems man and Cybernetics 9 (1979), 62–66.

[5] N. Tsapatsoulis P.Tzouveli, K. Ntalianis and S.Kollias, Automatic face region watermarking using qualified significant wavelet trees, Proceedings of 9th International Workshop on Systems, Signal and Image Processing,
Control Systems Centre Manchester, United Kingdom (November , 2002), 101–103.

[6] K. R. Ramakrishnan Saraju P. Mohanty and Mohan S Kankanahalli, An adaptive dct domain visible watermarking technique for protection of publicly avalaible images, ICMPS (2000).

[7] Wen Xing, A digital watermarking method based on classified labeled bisecting-k-means clustering, Proceedings of Second International Conference on Machine Learning and Cybernetics. (November-2003).

[8] Wenjun Zeng, Digital watermarking and datahiding: Technologies and applications, Proceedings of International Conference on Information System, Analysis and Synthesis. 3 (1999).

© 2010 ACEEE
DOI: 01.ijsip.01.01.03

ACEEE